

CYNTHIA A. HARDING, M.P.H.
Interim Director

JEFFREY D. GUNZE NHAUSER, M.D., M.P.H.
Interim Health Officer

313 North Figueroa Street, Room 708
Los Angeles, California 90012
TEL (213) 240-8156 • FAX (213) 481-2739

www.publichealth.lacounty.gov



BOARD OF SUPERVISORS

Hilda L. Solis
First District
Mark Ridley-Thomas
Second District
Sheila Kuehl
Third District
Don Knabe
Fourth District
Michael D. Antonovich
Fifth District

June 30, 2015


The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

ADOPTED

BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

28 June 30, 2015


PATRICK OZAWA
ACTING EXECUTIVE OFFICER

APPROVAL TO ENTER INTO DATA USE AGREEMENTS AND FUTURE AGREEMENTS AND/OR AMENDMENTS WITH THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL, CAROLINA POPULATION CENTER, AND WITH THE CALIFORNIA DEPARTMENT OF PUBLIC HEALTH FOR THE VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM, EFFECTIVE FOR THREE YEARS UPON EXECUTION BY BOTH PARTIES (ALL SUPERVISORIAL DISTRICTS) 3 VOTES)

SUBJECT

Request approval to enter into a Data Use and Disclosure Agreement and future agreements and/or amendments with The University of North Carolina at Chapel Hill, Carolina Population Center for the purpose of obtaining access to data from the National Longitudinal Study of Adolescent Health, and with the California Department of Public Health, for access to the Vital Records Business Intelligence System for the purpose of permitting the secure exchange of Statewide and County-Specific California Birth and Death Data Indices and Files.

IT IS RECOMMENDED THAT THE BOARD:

1. Approve and instruct the Interim Director of the Department of Public Health (DPH), or her designee, to execute a Data Use Agreement (DUA) (Exhibit I), with a provision for indemnification, from The University of North Carolina at Chapel Hill, Carolina Population Center (UNC) at a total maximum obligation estimated not to exceed \$850, offset by The California Endowment Health Impact Evaluation Center (HIEC) Grant, for the purpose of obtaining access to data from the National Longitudinal Study of Adolescent Health (Add Health), effective upon execution by both parties, but no sooner than Board approval, for a period of three years.
2. Approve and instruct the Interim Director of DPH, or her designee, to execute a no-cost Data Use and Disclosure Agreement (DUA) (Exhibit II), with a provision for indemnification, from the California

Department of Public Health (CDPH), for access to the Vital Records Business Intelligence System (VRBIS) for the purpose of permitting the secure exchange of Statewide and County-Specific birth and death data indices and files compiled by the State Registrar, effective upon execution by both parties, but no sooner than Board approval, for a period of three years.

3. Delegate authority to the Interim Director of DPH, or her designee, to execute future agreements and/or amendments that are consistent with the requirements of the DUAs referenced above that extend the term as determined by UNC and CDPH and/or reflect modifications to the DUAs as specified by UNC and CDPH, subject to review and approval by DPH's Division of Public Health Information Systems (PHIS) and County Counsel, and notification to your Board and the Chief Executive Office (CEO).

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Approval of Recommendation 1 will allow DPH to enter into a DUA with UNC for a three-year period to permit DPH's Office of Health Assessment and Epidemiology to produce a Health Impact Assessment (HIA) Report, which will outline the potential change in short- and long-term health outcomes due to truancy prevention programs, such as those led by the District Attorney and the City Attorney. A component of the HIA is the development of a model to estimate the academic, social, and health outcomes that could result from improved school attendance. Data from Add Health will be used to elucidate these relationships, which will assist in developing the model.

Add Health is a nationally representative sample of adolescents in grades 7-12 in the United States; this sample of respondents were followed in four waves: 1994-95, 1996, 2001-02, and 2007-08. The number of students who participated in Wave I of the in-home survey was 20,745. Data are available on the number of excused and unexcused absences reported by students in middle school. The Add Health study followed the middle school students for 13 years and provides data on basic demographic information; educational and employment attainment; crime and delinquency; tobacco, alcohol, and drug use; general health; nutrition; pregnancy; public assistance; risky sexual behaviors; number of drop outs; and general school level variables.

In accordance with Exhibit I, the County agrees to indemnify, defend, and hold harmless The University of North Carolina at Chapel Hill, Add Health, and the sources of Sensitive Data from any or all claims and losses accruing to any person, organization, or other legal entity as a result of County's acts, omissions, or breaches of the Agreement.

Approval of Recommendation 2 will allow DPH to enter into a DUA with CDPH for a three-year period to permit the secure exchange of birth, death, and fetal death data used by DPH. CDPH and its Director, designated in statute as the State Registrar, pursuant to Division 102 of the California Health Safety Code (H&SC), is charged with the duties of registering, maintaining, indexing, and issuing certified copies of all California birth, death, and fetal death records. As part of these activities, the State Registrar operates VRBIS database. VRBIS is a secure, web-based electronic database for the State Registrar to store California's vital records data. This system permits local health departments to access such data for purposes of official government business including epidemiologic analysis, surveillance, and program evaluation, as directed by the Local Health Officer, following all applicable laws and regulations concerning vital records data.

To obtain the VRBIS data, the executed DUA must be on file with CDPH to ensure that both parties are in compliance with all State and federal laws applicable to the protected data (i.e. birth, death,

and fetal death data). These data include personal and protected information and are the primary source of protected data used.

In accordance with Exhibit II, the County shall indemnify, hold harmless, and defend CDPH from and against any and all claims, losses, liabilities, damages, costs, and other expenses (including attorney's fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Data Recipient, its officers, employees, or agents relative to the Protected Data, including without limitation, any violations of Data Recipient's responsibilities under the Agreement. County Counsel, PHIS, and CEO Risk Management have reviewed and approved Exhibit I and Exhibit II as to use.

Approval of Recommendation 3 will allow DPH to execute future agreements and/or amendments that extend the term and/or reflect modifications to the DUAs as specified by UNC and CDPH.

Implementation of Strategic Plan Goals

The recommended actions support Goal 3, Integrated Services Delivery, of the County's Strategic Plan.

FISCAL IMPACT/FINANCING

The total cost for the DUA between DPH and UNC is estimated not to exceed \$850; 100 percent funded by The California Endowment HIEC Grant. Funds will be used to cover the expenses of producing and shipping data files and codebooks, consulting, and administering the DUA.

The no-cost DUA between CDPH and DPH has no fiscal impact.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

Add Health was developed in response to a mandate from the U.S. Congress to fund a study of adolescent health that focuses on forces which may influence adolescents' health and risk behaviors. It has become a national data resource for over 10,000 researchers. Through the Add Health dataset, recommendations, policy development, and program planning will result in a report addressing chronic truancy through early intervention strategies.

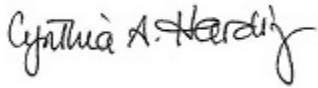
CDPH is responsible for oversight of the registration of births, deaths, and fetal deaths in California and Los Angeles County and, as such, presently maintains and utilizes the Automated Vital Statistics System (AVSS) and the Electronic Death Registration System (EDRS). VRBIS is a new secure, web-based electronic solution for the State Registrar to store California's vital records data and to permit local health departments to access such data.

DPH implements administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of confidential, protected health information. All confidential, protected health information is stored on encrypted systems and access to all systems requires authorized users to authenticate their identity with a unique username and password.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommended actions will allow DPH to enter into a three-year DUA with UNC to access data to study short- and long-term health outcomes due to truancy prevention programs. It will also allow DPH to enter into a three-year DUA with CDPH for the continued secure exchange of birth, death, and fetal death data used by national, State, and local stakeholders for policy development, program planning, and epidemic monitoring.

Respectfully submitted,

A handwritten signature in cursive script that reads "Cynthia A. Harding".

Cynthia A. Harding, M.P.H.

Interim Director

CAH:jc
BL # 03201

Enclosures

c: Interim Chief Executive Officer
County Counsel
Acting Executive Officer, Board of Supervisors

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

General Information and Checklists

***Please read the entire package and return this completed checklist
to ensure that you have included all of the required contract forms and supporting documents.***

Checklist for contract forms

- ☐ Investigator Information
- ☐ Agreement for the Use of Restricted-Use Data
- ☐ Investigator and Institutional Signatures Page
- ☐ Attachment A: Sensitive Data Security Plan
- ☐ Attachment B: Data File Order Form
 - ☐ Include explanations for requested constructed datasets
- ☐ Attachment C: Supplemental Agreement with Research Staff
signed by Investigator and each Research Staff person
- ☐ Attachment D: Security Pledge(s) – one for each Research Staff person, signed
- ☐ Attachment E: List of Funding Agencies
- ☐ Attachment F: Description of Deductive Disclosure Risk

Checklist for supporting documents

- ☐ IRB approval of Sensitive Data Security Plan and the research project
- ☐ Nonrefundable processing fee (\$850) payable by check to "The University of North Carolina at Chapel Hill" and sent to the address below

A FULLY EXECUTED CONTRACT WILL BE RETURNED TO YOU UPON APPROVAL.

Please allow a minimum of four weeks for processing.

Send completed package to:

Add Health
The University of North Carolina at Chapel Hill
Carolina Population Center
206 West Franklin Street
Chapel Hill, NC 27516-2524

Contact:

Kayla Sauls
Email: addhealth_contracts@unc.edu

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Investigator Information

DATE	
NAME OF INVESTIGATOR	Ricardo Basurto-Davila
INVESTIGATOR'S DEGREE	PhD
INVESTIGATOR'S POSITION	Health Economist
INVESTIGATOR'S INSTITUTION	Los Angeles County Department of Public Health
DEPARTMENT	Office of Health Assessment and Epidemiology
STREET ADDRESS	Note: Because data CDs will be shipped by 2 nd -day traceable delivery, we cannot accept P.O. BOXES. 313 N Figueroa St, Room 127
CITY/STATE/ZIP CODE	Los Angeles, CA 90012
TELEPHONE	213-989-7127
FAX	213-250-2594
EMAIL	RBasurto@ph.lacounty.gov
TITLE OF RESEARCH PROJECT	Truancy HIA: Truancy Intervention Model to Predict Short-and Long-Term Health Outcomes

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Agreement for the Use of Restricted-Use Data

I. Definitions

- A. "The National Longitudinal Study of Adolescent Health" (hereinafter referred to as "Add Health") is the program project undertaken by the Carolina Population Center of The University of North Carolina at Chapel Hill (hereafter referred to as UNC-Chapel Hill) under Grant No. P01-HD31921 from the Eunice Kennedy Shriver National Institute of Child Health and Human Development.
- B. "Investigator" is the person primarily responsible for supervision of the research project, security of the data, and use of sensitive data obtained through this Agreement.
- C. "Research Staff" are all persons, excluding Investigator, who will have access to sensitive data obtained through this Agreement.
- D. "Institution" is the university or research institution that employs Investigator and that is the signatory to this Agreement on behalf of Investigator.
- E. "Representative of Institution" is a person authorized to enter into contractual agreements on behalf of Institution.
- F. "Sensitive Data" includes any data from Add Health that might compromise the anonymity or privacy of respondents to that study. Because of the school-based study design, Add Health respondents (adolescents, parents, and schools) are at higher risk of deductive disclosure than randomly sampled individuals. Therefore, all data collected from Add Health are considered to be sensitive.
- G. "Data File" includes any form of data, whether on paper or electronic media.
- H. "Funding Agency" is a federal office or institute that provided funding for Add Health. Funding agencies are only the offices or institutes providing the funding; other divisions or institutes within the larger organization are not considered funding agencies.
- I. "Contract Period" is the three (3)-year period that begins and ends on the dates specified on page 11 .
- J. "Processing Fee" is a nonrefundable payment of \$850 that covers the expenses of producing and shipping Data Files and codebooks, of consulting, and of administering this Agreement.

II. Requirements of Investigators

Investigators must meet the following criteria:

- A. Have a PhD or other terminal degree; and
- B. Hold a faculty appointment or research position at Institution

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

III. Requirements of Institution

Institution must meet the following criteria:

- A. Be an institution of higher education, a research organization, or a government agency
- B. Have a demonstrated record of using sensitive data according to commonly accepted standards of research ethics

IV. Obligations of Add Health

In consideration of the promises made in Section V of this Agreement and of receipt of the monies noted in Section V. I., Add Health agrees to the following, once a copy of the completed contract has been received and Attachment A has been approved:

- A. To submit for review by the appropriate officials of UNC-Chapel Hill the original of this Agreement.
- B. To return one fully signed original to Investigator by first-class mail.
- C. To assign the effective dates of the three (3)-year Contract Period on the Institutional Signatures page. The initiation date will be within 15 working days of receipt of the signed originals from appropriate UNC-Chapel Hill officials.
- D. To provide the Data Files requested by Investigator in the Data File Order within a reasonable time frame following execution of this Agreement by appropriate officials of UNC-Chapel Hill and to send the requested Data Files to Investigator on a CD-ROM by second-day trackable delivery. All Data Files will be compressed and encrypted.
- E. To provide codebooks which contain the origins, form, and general content of the Data Files sent to Investigator within the same time frame and manner as specified in paragraph D regarding the Data Files.
- F. To provide one (1) hour of consultation to Investigator and/or Research Staff regarding the origins, form, and general content of the Data Files, and regarding required and preferred techniques for data management of those Data Files. Further consultation is available for an additional fee.

V. Obligations of the Investigator, Research Staff, and Institution

Data provided under this Agreement shall be held by the Investigator, Research Staff, and Institution in strictest confidence and can be disclosed only in compliance with the terms of this Agreement.

In consideration of the promises contained in Section IV of this agreement, and for use of Data Files from Add Health, the Investigator, Research Staff, and Institution agree:

- A. That the Data Files will be used solely for statistical analyses: that no attempt will be made to identify specific individuals, families, households, schools, institutions, or geographic locations not provided by Add Health; and that no list of Sensitive Data at the individual or family level will be published or otherwise distributed.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- B. That if the identity of any person, family, household, school, institution or geographic location should be discovered inadvertently, then:
 - 1. No use will be made of this knowledge;
 - 2. Add Health will be advised of the incident within one (1) business day of Investigator's, Research Staff's, or Institution's discovery of the incident;
 - 3. The information that would identify the person, family, household, school, or institution will be safeguarded or destroyed as requested by Add Health and a written certification of destruction provided to Add Health; and
 - 4. No one else will be informed of the discovered identity.
- C. To avoid inadvertent disclosure of persons, families, or households by using the following guidelines in the release of statistics derived from the Data Files.
 - 1. In no table should all cases in any row or column be found in a single cell.
 - 2. In no case should the total for a row or column of a cross-tabulation be fewer than three (3).
 - 3. In no case should a cell frequency of a cross-tabulation be fewer than three (3) cases.
 - 4. In no case should a quantity figure be based on fewer than three (3) cases.
 - 5. Data released should never permit disclosure when used in combination with other known data.
- D. That no persons other than those identified in this Agreement, or in amendments subsequent to this agreement, as Investigator or Research Staff, be permitted access to the contents of Data Files or any files derived from sensitive Data Files.
 - 1. That within one (1) business day of becoming aware of any unauthorized access, use, or disclosure of Sensitive Data, the unauthorized access, use, or disclosure of Sensitive Data will be reported in writing to Add Health.
- E. To comply fully with the Sensitive Data Security Plan, which is included as Attachment A to this Agreement. The Sensitive Data Security Plan expires at the end of the Contract Period.
- F. To respond fully and in writing within ten (10) working days after receipt of any inquiry from Add Health regarding compliance with this Agreement or the expected date of completion of work with the Sensitive Data and any data derived therefrom.
- G. To make available for inspection by Add Health, during business hours, the physical housing and handling of all Data Files and any other information, written or electronic, relating to this Agreement.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- H. To supply Add Health with a copy of each of the following:
1. Investigator Information form
 2. Agreement for the Use of Sensitive Data, each with original Institutional Signatures page
 3. Sensitive Data Security Plan (Attachment A)
 4. Data File Order with specific files requested, and explanatory statements for constructed datasets (if requested) (Attachment B)
 5. Supplemental Agreement with Research Staff for the Use of Sensitive Data signed by each Research Staff person (Attachment C)
 6. Security Pledges for the Investigator and each Research Staff person (Attachment D)
 7. List of Funding Agencies (Attachment E)
 8. Description of Deductive Disclosure Risk (Attachment F)
 9. A copy of the document, originated by the Investigator and signed by Institution's Institutional Review Board (IRB), approving the research project AND the secure use, storage, and handling of the Add Health Data Files outlined in the Sensitive Data Security Plan.
- I. To provide to UNC-Chapel Hill a nonrefundable processing fee in the amount of \$850. Payment may be made by check, payable to "The University of North Carolina at Chapel Hill." The nonrefundable processing fee will be used to cover the expenses of producing and shipping Data Files and codebooks, of consulting, and of administering this Agreement.
- An exemption to the nonrefundable processing fee may be made if the request for Data Files is from an Investigator at one of the Add Health funding agencies or institutes. To request a waiver of the nonrefundable processing fee, please include a letter from the head of the funding agency requesting that the fee be waived.
- J. To include in each written report or other publication based on analysis of Sensitive Data from Add Health, the following statement:

This research uses data from Add Health, a program project designed by J. Richard Udry, Peter S. Bearman, and Kathleen Mullan Harris, and funded by a grant P01-HD31921 from the Eunice Kennedy Shriver National Institute of Child Health and Human Development, with cooperative funding from 17 other agencies. Special acknowledgment is due Ronald R. Rindfuss and Barbara Entwisle for assistance in the original design. Persons interested in obtaining Data Files from Add Health should contact Add Health, The University of North Carolina at Chapel Hill, Carolina Population Center, 206 W. Franklin Street, Chapel Hill, NC 27516-2524 (addhealth_contracts@unc.edu). No direct support was received from grant P01-HD31921 for this analysis.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- K. That all journal articles based on analysis of Confidential Data from Add Health receive a PubMed Central reference number (PMCID). Journal articles must be submitted to PubMed Central to receive a PMCID. The method of PubMed Central submission and Investigator responsibility for submission depend on the journal and journal publisher.
1. Some journals automatically submit published articles to PubMed Central. For a list of journals that submit articles to PubMed Central please visit the NIH website: http://publicaccess.nih.gov/submit_process_journals.htm
 2. Some journal publishers may submit the articles to PubMed Central automatically or upon request by the author. For a list of journal publishers that submit articles to PubMed Central please visit the NIH website: http://publicaccess.nih.gov/select_deposit_publishers.htm#b
 3. If neither the journal nor the journal publisher will submit the article to PubMed Central, the Investigator will be responsible to submit the final peer-reviewed manuscript to PubMed Central via the NIH Manuscript Submission System (NIHMS). For detailed instructions on the process of submitting a journal article to PubMed Central, please see the NIH website: http://publicaccess.nih.gov/submit_process.htm
 4. If you have any problems with this process, please contact the NIHMS or PubMed help desk.
- L. To complete the following protocol upon separation from Institution or the expiration of Investigator's contract:
1. Destroy all Data Files at the originally approved site
 2. Submit a letter stating that all Add Health Data Files have been securely erased with the secure erasure program listed in the security plan for the originally approved site.
 3. Return all CDs containing Data Files, within thirty (30) days of the expiration of the Contract Period, as specified on the Institutional Signatures page, or to submit a renewal application.

Add Health shall be able to visit within a year of contract termination, to confirm the data have been destroyed. This obligation of destruction shall not apply to Investigator's scholarly work produced during the Contract Period that is based upon or that incorporates the Sensitive and Romantic Data.

- M. To notify Add Health in the event Investigator plans to separate from Institution during the Contract Period. Such notification must be in writing and must be received by Add Health at least six (6) weeks prior to Investigator's last day of employment with Institution. Investigator's separation from Institution will terminate this Agreement. Investigator may, however, reapply to receive Data Files from Add Health in Investigator's capacity as an employee of his or her new institution. No fee will be charged for the administration of this process.

Concurrent with Investigator's notice to Add Health regarding a pending separation from Institution, Investigator must:

1. Return the Data File CDs to Add Health at the following address:

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

Add Health
Carolina Population Center
206 W. Franklin St.
Chapel Hill, NC 27516-2524

2. Destroy all electronic and paper files at the originally approved site prior to the date of relocation and submit a letter stating that all Add Health files have been securely erased with the secure erasure program listed in the security plan for the originally approved site. This obligation of destruction shall not apply to Investigator's scholarly work produced during the Contract Period that is based upon or that incorporates the Sensitive Data.
- N. To obtain approval from Add Health prior to transferring this Agreement to another Investigator at the same Institution. No fee will be charged for the administration of this process. In order to obtain such approval, Investigator must:
1. Inform Add Health in writing six (6) weeks prior to the proposed date of transfer.
 2. Submit a complete copy of this Agreement in the name of the new Investigator signed by an official representative of Investigator's new institution.
 3. Maintain responsibility for the security of all Data File CDs until the transfer contract has been approved.
- O. To submit annual reports to Add Health on or before each anniversary of the initial date of the Contract Period. Such reports must include:
1. A copy of the annual IRB approval for the research project
 2. A list of public presentations at professional meetings using results based on the Data Files
 3. A list of papers accepted for publication using these Data Files, with complete citations
 4. A list of grants that have been awarded for use of the Add Health Data Files
 5. A list of graduate students using the Add Health Data Files for dissertations or theses, the titles of these papers, and the dates of completion
 6. A current data user roster including the names of all research staff member(s) who have access to Data Files and their relationship(s) to the project

Such reports shall be signed by Investigator. Add Health reserves the right to terminate this Agreement in the event that the reports are not timely submitted.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- P. That Investigator and Institution hereby acknowledge that any breach of the confidentiality provisions herein will result in irreparable harm to The University of North Carolina at Chapel Hill that are not adequately compensable by money damages. Investigator, Research Staff, and Institution hereby agree to the imposition of injunctive relief in the event of breach, in addition to money damages. Should Investigator, Research Staff, or Institution commit a material breach of this agreement that is not cured within thirty (30) days after Investigator or Institution receives notice of such breach from Add Health, Add Health reserves the right to terminate the Agreement, in which case all electronic and paper files will be securely erased; a letter will be submitted by the Investigator, stating that all Add Health files have been securely erased with the secure erasure program listed in the security plan; and CDs containing Data Files are to be returned. Investigator, Research Staff, and Institution understand and agree that a violation of any of the terms and conditions of this Agreement may constitute a violation of state and federal statutes and may subject Investigator, Research Staff, and/or Institution to the criminal, civil, and administrative penalties associated with violations of those statutes, in addition to constituting a material breach of this Agreement with attendant legal liabilities.
- Q. That Investigator and Institution agree to indemnify, defend, and hold harmless The University of North Carolina at Chapel Hill, Add Health, and the sources of Sensitive Data from any or all claims and losses accruing to any person, organization, or other legal entity as a result of Investigator's, Research Staff's and/or Institution's acts, omissions, or breaches of this Agreement.
- R. That Institution shall ensure that Research Staff comply with the provisions of this Agreement.

VI. Certificate of Confidentiality

Research subjects who participated in Add Health are protected by a certificate of confidentiality issued by the Department of Health and Human Services in accordance with the provisions of section 301(d) of the Public Health Service Act (42 U.S.C. § 241(d)). Institution is considered to be a contractor or cooperating agency of UNC-Chapel Hill under the terms of the Confidentiality Certificate; as such, Institution, Investigator, and Research Staff are authorized to protect the privacy of the individuals who are the subjects of Add Health by withholding their identifying characteristics from all persons not connected with the conduct of the study. Identifying characteristics are all Add Health Data Files which are defined as sensitive under the terms of this contract.

VII. Incorporation by Reference

The parties agree that the following documents are incorporated into this Agreement by reference:

- A. A copy of the IRB approval of the research project, taking into special consideration deductive disclosure risks.
- B. The Sensitive Data Security Plan proposed by Investigator and approved by Add Health.
- C. The Department of Health and Human Services Confidentiality Certificate, a copy of which will be sent with the signed contract.

VIII. Attachments

- A. Sensitive Data Security Plan for the Use of Restricted-Use Data from the National Longitudinal Study of Adolescent Health

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- B. Data File Order for the Use of Sensitive Data from the National Longitudinal Study of Adolescent Health
- C. Supplemental Agreement with Research Staff for the Use of Sensitive Data from the National Longitudinal Study of Adolescent Health
- D. Security Pledge for the Use of Sensitive Data from the National Longitudinal Study of Adolescent Health
- E. List of Funding Agencies for the National Longitudinal Study of Adolescent Health
- F. Description of Deductive Disclosure Risk from the National Longitudinal Study of Adolescent Health

IX. Miscellaneous

- A. The laws of North Carolina shall govern the validity and interpretation of the provisions, terms and conditions of the Agreement. In the event the parties are unable to resolve any dispute relating to this agreement, all suits, actions, claims, and causes of action relating to this Agreement shall be brought in the courts of the State of North Carolina.
- B. All notices, contractual correspondence, and return of data under this Agreement on behalf of the Investigator shall be made in writing and delivered to the address below:

Add Health
The University of North Carolina at Chapel Hill
Carolina Population Center
206 W. Franklin St.
Chapel Hill, NC 27516-2524
- C. Provisions of Data Files, all notices, and contractual correspondence under this Agreement on behalf of Add Health shall be made in writing and delivered to Investigator at the address listed on the Institutional Signatures page.
- D. This Agreement shall be effective for the dates indicated on the Institutional Signatures page.
- E. The respective rights and obligations of Add Health and Investigator, Research Staff, and Institution pursuant to this Agreement shall survive termination of this agreement.
- F. In the event of a material breach of this Agreement by the Investigator, Research Staff, or Institution, Add Health may terminate this Agreement by providing written notice to Investigator and Institution. In this event, Add Health will not be required to refund of any portion of the nonrefundable \$850 processing fee.
- G. This Agreement may be amended or modified only by the mutual written consent of the authorized representatives of Add Health and Investigator and Institution. Both parties agree to amend this Agreement to the extent amendment is necessary to comply with the requirements of any applicable regulatory authority.
- H. This Agreement contains all of the terms and conditions agreed upon by the parties regarding the subject matter of this Agreement and supersedes any prior agreements, oral or written, and all other communications between the parties relating to such subject matters.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Agreement for the Use of Restricted-Use Data
(continued)**

- I. The persons signing this Agreement have the right and authority to execute this Agreement, and no further approvals are necessary to create a binding agreement.
- J. The obligations of Investigator, Research Staff, and Institution set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of Add Health.
- K. Add Health's existing ownership rights in its intellectual property, including its Sensitive Data and the Data Files, are not affected by this Agreement. Except as expressly set forth herein, no right, license, title, or interest in any of Add Health's intellectual property or in any invention, process, or product arising out of its intellectual property is granted or implied, whether or not patented or patentable.
- L. This Agreement may be executed in one or more counterparts each of which counterpart shall be deemed an original Agreement and all of which shall constitute but one Agreement.
- M. The parties' electronic signatures shall be the legally binding equivalent of a handwritten signature.
- N. Institution hereby appoints Investigator as its designated representative to execute, on behalf of Investigator and Institution, additional forms pursuant to this Agreement. Such forms include Attachments A, B, C, and D.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Investigator and Institutional Signatures

Investigator

Institutional Representative

SIGNATURE _____ DATE _____

Ricardo Basurto-Davila

SIGNATURE _____ DATE _____

Cynthia A. Harding

NAME TYPED OR PRINTED _____

Health Economist

NAME TYPED OR PRINTED _____

Interim Director

TITLE _____

Los Angeles County Department of Public Health 

TITLE _____

Los Angeles County Department of Public Health

INSTITUTION _____

313 N Figueroa Street Room 127

INSTITUTION _____

313 North Figueroa Street Room 708

BUILDING ADDRESS _____

BUILDING ADDRESS _____

STREET ADDRESS _____

Los Angeles, CA 90012

STREET ADDRESS _____

Los Angeles, California 90012

CITY, STATE ZIP _____

CITY, STATE ZIP _____

Representative of Add Health

Representative of UNC-CH

SIGNATURE _____ DATE _____

Kathleen Mullan Harris
Principal Investigator
Carolina Population Center
206 West Franklin Street
Chapel Hill, NC 27516-2524

SIGNATURE _____ DATE _____

for Barbara Entwisle
Vice Chancellor for Research
University of North Carolina at Chapel Hill
Chapel Hill, NC 27599-1350

For Add Health Use Only:

Security Plan & Contract Period: _____ through _____

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Instructions for Completing Attachment A: Sensitive Data Security Plan

Below are a number of different locations where you might choose to store the Add Health data. Please make your selection and then read the associated document "How to secure ..." from our web site to see the essential components of a good security plan for that location. Submit the completed Attachment A: Form to Describe Sensitive Data Security Plan for your location.

If your location is not listed, or if you need assistance with the security plan, please email addhealth@unc.edu.

Data Stored on a Stand-Alone Computer

A stand-alone computer is one that is in no way connected to another computer or networked device such as a switch, hub, or router.

The security plan form and information on how to secure a stand-alone computer are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/standalone>.

Data Stored on an External Hard Drive

The external hard drive is a modified version of the stand-alone computer, in effect keeping the Add Health data off the Internet or a local area network (LAN).

The security plan form and information on how to secure an external hard drive are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/externaldrive>

Data Stored on a Computer Connected to a Private Network

A private network is two or more computers and/or network devices (e.g., printer, switch, hub, router) that are not connected in any way to the Internet or a LAN.

The security plan form and information on how to secure a computer connected to a private network are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/privatenetwork>

Data Stored on a Windows Computer Connected to Network

A network is two or more computers and/or network devices (e.g., printer, switch, hub, router) that are connected to the Internet or a LAN.

The security plan form and information on how to secure a Windows computer connected to a network are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/windowsnetwork>

Data Stored on a Macintosh Computer Connected to Network

A network is two or more computers and/or network devices (e.g., printer, switch, hub, router) that are connected to the Internet or a LAN.

The security plan form and information on how to secure a Macintosh computer connected to a network are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/macnetwork>

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

**Instructions for Completing Attachment A: Sensitive Data Security Plan
(continued)**

Data Stored on a Windows Server

Because the Windows server is connected to the Internet or to a local or wide area network, the emphasis for securing the data on this server is placed on physical security of the server, controlling access to the data, and protecting the data from unauthorized access across the wire.

The security plan form and information on how to secure a Windows server are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/win2000server>

Data Stored on a NetWare Server

Because the NetWare server is connected to the Internet or to a local or wide area network, the emphasis for securing the data on this server is placed on physical security of the server, controlling access to the data, and protecting the data from unauthorized access across the wire.

The security plan form and information on how to secure a NetWare server are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/netwareserver>

Data Stored on a Unix or Linux Server

Guidelines for securing a server that is running a version of the Unix or Linux operating system.

The security plan form and information on how to secure a Unix or Linux server are available at <http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/unixlinux>

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment B: Data File Order Form

- Data will be delivered as a SAS export file.
- Data will be sent on a CD by second day, traceable delivery and the Investigator will be notified by email when the data are shipped.
- All data files will be compressed and encrypted.
- Codebooks will be delivered in electronic form on a CD.

Ricardo Basurto-Davila

CONTACT PERSON

RBasurto@ph.lacounty.gov

CONTACT PERSON'S EMAIL

Ricardo Basurto-Davila

INVESTIGATOR'S NAME

INVESTIGATOR'S SIGNATURE

DATE OF SIGNATURE

The following data will be sent automatically, upon execution of your contract:

In-home Interview Files

- Wave I
- Wave II
- Wave III
- Wave IV

School Files

- Wave I School Administrator
- Wave II School Administrator
- School Information
- In-School Questionnaire

Weight Files

- Wave I Grand Sample Weights
- Wave II Grand Sample Weights
- Wave III Grand Sample Weights
- Wave IV Grand Sample Weights
- School Administrator Weights
- In-School Weights

The constructed datasets listed below are available by special request.

*In order to receive one or more of these datasets,
please attach a brief statement explaining the necessity and relevance of the data to your research agenda.*

School Files

- ☒ School Network
- ☒ Network Structure

Friend Files

- ☐ In-School Nominations
- ☐ Wave I In-Home Nominations
- ☐ Wave II In-Home Nominations
- ☐ Wave III Friend IDs

Sibling Files

- ☒ Adolescent Pair Data
- ☒ Wave III Sibling IDs

Contextual Files

- ☒ Wave I Contextual
- ☒ Wave II Contextual
- ☒ Wave III Contextual
- ☒ Wave I Neighborhood
- ☒ Wave II Neighborhood
- ☒ Wave III Grouping
- ☒ Wave IV Grouping
- ☒ Wave I Spatial
- ☒ Wave III Census Region
- ☒ Wave IV Census Region
- ☒ Wave III Tract-Level
- ☒ Wave IV Tract-Level

Wave III Supplemental Files

- ☐ Urinalysis
- ☐ ASHA Call
- ☐ HPV MGEN
- ☒ Mentor Codes
- ☒ BEM Scores
- ☐ Cotinine

Weight Files

- ☒ Wave I Weight Components
- ☒ Wave II Weight Components
- ☒ Wave III Weight Components
- ☒ Wave IV Weight Components
- ☒ In-School Weight Components
- ☒ Add Health School Weights
- ☐ HPV MGEN Weights

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment B: Data File Order Form

Education Files (Wave III)

- ☒ Academic Courses
- ☒ Academic Networks
- ☒ Context
- ☒ Course Level
- ☒ Curriculum
- ☒ Linking
- ☒ Primary
- ☒ Transition
- ☒ Weights

Genetic Files

- ☐ Wave III DNA Results
- ☐ Wave IV DNA Results

Constructed Variables

- ☒ Wave IV Constructed

Disposition Files

- ☒ Wave I Disposition
- ☒ Wave II Disposition
- ☒ Wave III Disposition
- ☒ Wave IV Disposition
- ☒ National Death Index

Obesity and Neighborhood

Environment (ONE)

- ☒ Wave I Climate
- ☒ Wave III Climate
- ☐ Wave I Street Connectivity
- ☐ Wave III Street Connectivity
- ☒ Wave I Crime
- ☒ Wave III Crime
- ☐ Wave I Geocode Source
- ☐ Wave III Geocode Source
- ☐ Wave I Land Cover
- ☐ Wave III Land Cover
- ☒ Wave I Parks
- ☒ Wave III Parks
- ☐ Wave I Urban Distances
- ☐ Wave III Urban Distances

☒ Wave I Resources

☒ Wave III Resources

☐ Wave I Weather

☐ Wave III Weather

☒ Wave I ACCRA Cost of
Living Index

☒ Wave III ACCRA Cost of
Living Index

☒ Wave I Employment

☒ Wave III Employment

☐ Wave I Length of Day

☐ Wave III Length of Day

☐ Wave I Road Type Length

☐ Wave III Road Type Length

☐ Wave I Rural-Urban

Commuting Area (RUCA)

☐ Wave III Rural-Urban

Commuting Area (RUCA)

☒ Wave I 1990 Population Density

☒ Wave III 2000 Population
Density

☒ Wave I School Distance

Measures

☒ Wave I Grouping

☒ Wave III Mobility

☐ Wave III MSA

Alcohol Density Files

- ☐ Wave III Alcohol Outlet Density

Political Context Files

☒ Wave I Political Context Data

☒ Wave II Political Context Data

☒ Wave III Political Context Data

Biomarker Data (Wave IV)

☐ Prescription Medication Use

☐ Glucose

☐ Measures of EBV and hsCRP

☐ Biomarker Consent

☒ Lipids

☐ Baroreceptor Sensitivity

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

Wave I In-home—A merged file containing the Wave I In-home Interview data, the Parent Questionnaire data (when available), the In-school Questionnaire data (when available), and the Add Health Picture Vocabulary Test (when available), collected in 1994-1995, weights included.

Wave II In-home—Data collected during the 1996 in-home interview, and weights included.

Wave III In-home—Respondent-level data collected during the 2001-2002 in-home interview includes field interviewer characteristics, AHPVT, and weights.

Wave IV In-home—The Wave IV in-home interview file includes the Wave IV interview data and interviewer demographic information.

Wave I School Administrator—Information from the Wave I self-administered questionnaire answered by an administrator at the school.

Wave II School Administrator—Information from the Wave II phone-administered interview answered by an administrator at the school.

School Information—Additional information about the individual schools.

In-school Questionnaire—Adolescent responses to the In-school Questionnaire administered September 1994 through April 1995.

School Files

School Network—Network variables constructed from the in-school questionnaire data and friendship nominations.

Network Structure—For each school pair, these files contain a valued friendship network and information on sex, grade in school, race, school pair, and total number of nominations made, including those to non-matchable or out-of-school friends. The files are stored as arc/edge lists in the PAJEK.PAJ format. Information on this freely available network software is at <http://vlado.fmf.uni-lj.si/pub/networks/pajek/>

Friend Files

In-School Nominations—Identification numbers of the friends that the respondent nominated during the in-school questionnaire.

Wave I In-home Nominations—Identification numbers of the friends that the respondent nominated during the Wave I in-home interview.

Wave II In-home Nominations—Identification numbers of the friends that the respondent nominated during the Wave II in-home interview.

Wave III Friend IDs—In Wave III, respondents in the 7th or 8th grade at Wave I were asked to identify, from a list of 10 computer-generated names, which ones were current friends or which ones were their friends when they were in school together. This dataset contains the IDs of the 10 computer-generated names.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

(continued)

Sibling Files

Adolescent Pair Data—Information that links and describes the sibling pairs.

Wave III Sibling IDs—In Wave III, respondents were asked questions about their siblings who also participated in the Wave I or II in-home interviews; this dataset contains the IDs for these siblings.

Contextual Files

Waves I, II and III Contextual—Community contextual variables based on state, county, tract, and block group levels derived from the Waves I, II and III addresses.

Waves I and II Neighborhood—Pseudo state, county, tract, and block group variables that allow respondents to be aggregated geographically based on Waves I and II addresses.

Waves III and IV Grouping—The pseudo FIPS codes in this file allow you to geographically group respondents by their Wave IV locations.

Wave I Spatial—X, Y coordinates that can be used to calculate distances between friends in a school community.

Waves III and IV Region—This file contains the Census region codes for the respondents' Wave III and IV residential locations.

Wave III Supplemental Tract-Level Contextual—This file contains supplemental Wave III contextual data that include transportation and commuting measures, climate descriptors, amenities, and state-level tobacco control influences. These variables are available at the census tract-level unless otherwise specified.

Wave IV Supplemental Tract-Level Contextual—This file contains tract-level measures, based on the Wave IV respondent locations, reported by the U.S. Census Bureau's 2009 American Community Survey (ACS), the Climate Atlas of the United States, the USDA Economics Research Service, Esri Data and Maps, ImpacTeen Tobacco Control Policy and Prevalence Data, and the Uniform Crime Reports. When tract-level measures were not available or appropriate, state and county level variables were used.

Wave III Supplemental Files

Urinalysis—This file contains nitrate, specific gravity, pH level, white blood cells, protein, glucose, ketone, urobilinogen, bilirubin, microalbumin, urine creatinine, and blood values from the Wave III urine specimens.

ASHA Call—To receive the results of their STD assays, Wave III respondents called an Add Health dedicated number at the American Social Health Association. This file provides information on who called the results hotline and the date and time of the call.

HPV MGEN—Assay results for human papillomavirus and mycoplasma genitalium are available for a subset of the Wave III respondents who provided a urine sample.

Mentor Codes—For Wave III respondents who reported having a mentor, the open-ended responses to the question "How did {HE/SHE} help you?" have been coded and are available in this file.

BEM Scores—The masculinity and femininity raw and standard scores from the 30 item short form BEM Sex-Role Inventory are available in this file.

Cotinine—This file contains the cotinine and 3-hydroxycotinine assay values for 963 Wave III respondents.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

(continued)

Weight Files

Weight Components—A weight component for each level of sampling (school and adolescents) has been created for each wave of data collection. This file contains the weight components needed for computing multilevel weights.

HPV MGEN Weights—Sample weights for respondents with HPV and MGEN assay results are in this file.

Education Files

Academic Courses—These files contain academic status and/or performance indicators for math, science, foreign language, English, history, social sciences, physical education, and a combined overall category.

Academic Networks—The Network files provide information on social networks based on the respondents' course-taking patterns.

Context—School level contextual data are from the Common Core of Data (CCD), Private School Survey (PSS), the 1990 and 2000 Census, and the Office of Civil Rights.

Course-Level—The data in this file are needed for merging the course-level curriculum data with other Education Files.

Curriculum—These math and science curriculum data are derived from coding the textbooks schools reported using for each course offered in these two subjects.

Linking—This file contains variables designed to link transcript data to academic or school years and to Add Health.

Primary—The Primary Component contains several types of indicators based on information collected from participating schools and listed directly on student transcripts such as student exit or graduation status and materials gathered from schools during the data collection process.

Transition—This file contains variables explaining the respondents' movement through the educational system.

Weights—This file contains weights for the education data along with the school weights needed for HLM analyses.

Genetic Files

Wave III DNA Results—Twin and full siblings interviewed at Wave III were asked to provide saliva samples for DNA analysis. This file contains the genotype values for DAT1 (dopamine transporter), DRD4 (dopamine receptor), and SLC6A4 (serotonin transporter), MAOA_V (monoamine oxidase A-uVNTR), DRD2 (dopamine D2 receptor), and CYP2A6 (cytochrome P450 2A6) from these samples. Also included are values for the following SNPs: rs2304297, rs892413, rs4950, rs13280604.

Wave IV DNA Results—The Wave IV DNA Data File contains genotyping results for all Wave IV respondents who agreed to provide a saliva sample for DNA testing. This dataset has values for DAT1 (dopamine transporter), DRD4 (dopamine receptor), MAOA (monoamine oxidase A- uVNTR), 5HTTLPR (serotonin transporter), HTTLPR La-Lg-S, and triallelic activity bins for the serotonin transporter 5HTTLPR adjusted for rs25531, catechol o-methyltransferase (rs4680), DRD2 (dopamine receptor D2), DRD5 (dopamine receptor D5), MAOCA1 (monoamine oxidase A dinucleotide repeat), and serotonin transporter (rs12945042).

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

(continued)

Disposition Files

Wave I and II Disposition File— Participation information for the Wave I in-home interview respondents and outcome data on the Wave II fielded cases.

Wave III Disposition File— Outcome information on the Wave III fielded cases.

Wave IV Disposition File— Outcome information on the Wave IV fielded cases.

National Death Index—Cause of death for the cases reported deceased at Waves III and IV are in this file.

Constructed Variables

Wave IV Constructed Variables— Wave IV constructed variables on personality, stress, depression, smoking, drinking, sexual activity, health, and economics.

The Obesity and Neighborhood Environment (ONE)

Wave I and III Climate— This file contains climate data for each Wave I and Wave III respondent based on the nearest climate station. Information is available on precipitation, total snowfall, sky cover, temperature, and total hours of sunshine.

Wave I and III Street Connectivity—These files contain road network connectivity measures within 1, 3, 5, and 8.05 km (5 miles) of the Wave I and III respondent locations.

Wave I and III Crime—The county level crime data in these files are based on the Wave I and III respondent locations.

Wave I and III Geocode Source—The data sources of the Wave I and III respondent residential geocodes (latitude and longitude) are provided in these files.

Wave I and III Land Cover—These files contain land cover metrics within 1, 3, 5, and 8.05 km (5 miles) of each respondent's location.

Wave I and III Parks—The counts of public parks within a Euclidean distance of 1, 3, 5, and 8.05 km (5 miles) of each respondent at Wave I and III are in these files.

Wave I and III Resources—The Add Health files provide data on the presence of various physical activity (PA) resources situated near respondent residences at Wave I and III.

Wave I and III Urban Distances—W1URBDST contains Euclidean distances to both 1990 and 2000 U.S. Census Urbanized Areas (UAs) for each Wave I respondent. W3URBDST contains the Euclidean distance to 2000 U.S. Census-Bureau-defined urbanized areas (UAs) for each Wave III respondent.

Wave I and III Weather—This file contains weather data for each Wave III respondent based on the nearest weather station reporting data for the correspondent survey month and year.

Wave I and III ACCRA Cost of Living Index—These Add Health Data Files contain ACCRA Cost of Living Index based on the location of the Wave I and Wave III respondents.

Wave I and III Employment—These Data Files contain county-level employment data attached to each Wave I and Wave III respondent location.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

(continued)

Wave I and III Length of Day—These Data Files contain the number of hours of daylight at each Wave I and Wave III respondent location on that respondent's survey date.

Wave I and III Road Type Length—These Data Files contain road type length calculations within radii of 1, 3, 5, and 8.05 kilometers (5 miles) of Wave I and Wave III respondent locations.

Wave I and III Rural-Urban Commuting Area (RUCA)—These Data Files contain Rural-Urban commuting area (RUCA) codes at the U.S. Census tract-level based on the location of Wave I and Wave III respondents.

Wave I and III Population Density—The Wave I population density file contains the proportion of 1990 U.S. Census block group population and area (in square meters) within 1, 3, 5, and 8.04672 km (5 mi) of each Wave I respondent. The Wave III population density file contains the proportion of 2000 U.S. Census block group population and area (in square meters) within 1, 3, 5, and 8.04672 km (5 mi) of each Wave III respondent.

Wave I School Distance Measures—The file contains the distance between the geocoded point locations of each respondent's Wave I location and that respondent's school.

Wave I Grouping—This Wave I grouping file is for use with the Obesity and Neighborhood Environment (ONE) data. The Wave I data in the ONE contextual files were created using these Wave I respondent locations. The grouping variable in this file is based on the Census FIPS codes and is a pseudo code, not linkable to outside data sources.

Wave III Mobility—W3MOBIND reports the distance between each respondent's geocoded point location for each survey wave and that respondent's school location, along with the respondent's move distance between each survey wave.

Wave III MSA Pseudo Codes—The MSA pseudo code created for each respondent's Wave III location is in this file.

Alcohol Density Files

Wave III Alcohol Outlet Density—This Add Health Data File measures the prevalence of alcohol outlets in respondent communities by reporting the tract-level density of establishments possessing on-and/or off-premise alcohol licenses.

Political Context Files

Wave I, II, III Political Context Data—The Add Health Political Context Database provides an array of measures that describe the political environments in which Add Health respondents reside. These contextual variables include measures of commuting, election results for gubernatorial, presidential, and senatorial races, and voter registration law.

Wave IV Biomarker Data

Prescription Medication Use—The files contained in this component of the Add Health restricted data include the type of medication used by participants during Wave IV.

Glucose—This file contains two measures of glucose homeostasis based on the assay of the Wave IV dried blood spots.

EBV and hsCRP Data—The results of the assays for CRP (C-reactive protein) and EBV (Epstein-Barr virus) are in this Data File.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Description of Data Files

(continued)

Biomarker Consent—In this file are variables indicating the types of consent (archive, no archive, refused, incarcerated) obtained for the Wave IV blood spot and saliva DNA collections.

Lipids—The Lipids data file contains measures of triglycerides (TG), total cholesterol (TC), high-density lipoprotein cholesterol (HDL-C), low-density lipoprotein cholesterol (LDL-C), non-high-density lipoprotein cholesterol, and total cholesterol to high-density lipoprotein cholesterol ratio.

Baroreceptor Sensitivity—This file contains constructed measures for baroreflex sensitivity, heart rate recovery, and systolic blood pressure recovery for the Wave IV respondents.

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment C: Supplemental Agreement with Research Staff

- I. The undersigned Research Staff, in consideration of their use of sensitive data from the National Longitudinal Study of Adolescent Health, agree:
 - A. That they have read the associated Agreement for the Use of Sensitive Data from the National Longitudinal Study of Adolescent Health and the Sensitive Data Security Plan.
 - B. That they are "Research Staff" within the meaning of the Agreement.
 - C. To comply fully with the terms of the Agreement, including the Sensitive Data Security Plan.
- II. The undersigned Investigator agrees that the persons designated herein are Research Staff within the meaning of the associated Agreement for the Use of Sensitive Data from the National Longitudinal Study of Adolescent Health.
- III. Investigator agrees to ensure that each Research Staff person signs this Supplemental Agreement and an individual Security Pledge (Attachment D).

Research Staff

Katherine Butler		
NAME TYPED OR PRINTED	SIGNATURE	DATE
Lauren Gase		
NAME TYPED OR PRINTED	SIGNATURE	DATE
Deena Pourshaban		
NAME TYPED OR PRINTED	SIGNATURE	DATE
Irene Vidyanti		
NAME TYPED OR PRINTED	SIGNATURE	DATE
NAME TYPED OR PRINTED	SIGNATURE	DATE
NAME TYPED OR PRINTED	SIGNATURE	DATE

Investigator

Ricardo Basurto-Davila		
NAME TYPED OR PRINTED	SIGNATURE	DATE

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment D: Security Pledge

Pledge of Confidentiality

I, Ricardo Basurto-Davila, through my involvement with and work on my project
TYPE OR PRINT YOUR NAME

will have access to Sensitive Data collected by the National Longitudinal Study of Adolescent Health (Add Health). By virtue of my affiliation with this project, I have access to Sensitive Data about respondents generally perceived as personal and private. I understand that access to this Sensitive Data carries with it a responsibility to guard against unauthorized use and to abide by the Sensitive Data Security Plan. To treat information as confidential means to not divulge it to anyone who is not a project member, or cause it to be accessible to anyone who is not a project member. Anything not specifically named as "public information" is considered confidential.

Disclosing confidential information from Add Health directly or allowing non-authorized access to such information may subject you to criminal prosecution and/or civil recovery and may violate the code of research ethics of your institution.

I agree to fulfill my responsibilities on this project in accordance with the following guidelines:

1. I agree not to permit non-project personnel access to these Sensitive Data, in either electronic or paper copy.
2. I agree to not attempt to identify individuals, families, households, schools, geographic locations or institutions.
3. I agree that in the event the identity of an individual, family, household, school, geographic location or institution is discovered inadvertently, I will (a) make no use of this knowledge, (b) advise the Investigator of the incident who will report it to Kathleen Mullan Harris within one (1) business day of discovery, (c) safeguard or destroy the information as directed by the Investigator after consultation with Kathleen Mullan Harris, and (d) not inform any other person of the discovered identity.

Location (Building and Room Number) of the Computer that will be used to access the Add Health

Restricted-Use data: 313 N Figueroa St, Room 127, Los Angeles CA 90012 +

Ricardo Basurto-Davila

NAME

SIGNATURE

DATE

Updates and corrections to the Add Health data and codebooks
will only be distributed through the Add Health list server.

EMAIL: RBasurto@ph.lacounty.gov

PROVIDE YOUR EMAIL ADDRESS TO SUBSCRIBE TO THIS LIST SERVER

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment E: List of Funding Agencies

National Cancer Institute

National Center for Health Statistics, Centers for Disease Control and Prevention, DHHS

National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, DHHS

National Center for Minority Health and Health Disparities

National Institute on Aging

National Institute of Allergy and Infectious Diseases

National Institute of Deafness and Other Communication Disorders

National Institute of General Medical Sciences

National Institute of Mental Health

National Institute of Nursing Research

National Institute on Alcohol Abuse and Alcoholism

National Institute on Drug Abuse

National Science Foundation

Office of AIDS Research, National Institutes of Health, NIH

Office of the Assistant Secretary for Planning and Evaluation, DHHS

Office of Behavioral and Social Science Research, NIH

Office of the Director, NIH

Office of Minority Health, Centers for Disease Control and Prevention, DHHS

Office of Minority Health, Office of Public Health and Science, DHHS

Office of Population Affairs, DHHS

Office of Research on Women's Health, NIH

**The University of North Carolina at Chapel Hill, Carolina Population Center
National Longitudinal Study of Adolescent Health
Restricted Use Data Contract**

Attachment F: Description of Deductive Disclosure Risk

The problem of deductive disclosure of an individual respondent's identity has become a major concern of federal agencies, researchers, and Institutional Review Boards in the recent past. In essence, deductive disclosure is the discerning of an individual respondent's identity and responses through the use of known characteristics of that individual. This is not unique to Add Health—if a person is known to have participated in ANY survey, then a combination of his or her personal characteristics will allow an individual to determine which record corresponds to that individual. For example, in the Add Health in-school dataset of more than 90,000 cases, a cross-tabulation of five variables can distinguish an individual record.

The Add Health data is more sensitive than many other datasets to deductive disclosure. This is due, in part, to the clustered research design. Add Health surveyed all students in grades 7 through 12 in a pair of schools in each of 80 communities in the United States. The in-school questionnaires were administered by teachers at each school. More than 120,000 students were enrolled in these schools. Informational letters were sent to parents prior to the administration date via students and post. Assuming that most students live with two other persons (parents and/or siblings), 360,000 people know of the participation of at least one, if not many, of the adolescents attending the selected schools. Additionally, approximately 5,000 school administrators, staff and teachers were involved in the in-school data collection efforts.

The in-home selection process increased the number of persons aware of Add Health: about 5,000 participants in the in-home component had not completed an In-School Questionnaire. (Participation in the in-school session was not a prerequisite for eligibility, only the presence of an adolescent's name on the school enrollment roster.)

Given the large number of people who know someone who, they know, participated in Add Health, researchers who use the Add Health Contractual Dataset are obligated to protect respondents from deductive disclosure risk by taking extraordinary precautions to protect the data from non-authorized use. Precautions include, but are not limited to: copying the original dataset only once and storing the original CD-ROM in a locked drawer or file cabinet; saving the computer programs used to construct analysis data files, but not the Data Files themselves; retrieving paper printouts immediately upon output; shredding printouts no longer in use; password protecting Add Health data; signing pledges of confidentiality; and using the data solely for statistical reporting and analysis.

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

This Data Use And Disclosure Agreement (hereinafter referred to as "Agreement") sets forth the information privacy and security requirements that the _____ Los Angeles County _____ Local Health Department (hereinafter "Data Recipient") is obligated to follow with respect to all Vital Records Business Intelligence System (VRBIS) data, and other personal and confidential information, (as each of these types of data and information are defined herein), disclosed to Data Recipient by the California Department of Public Health (CDPH). (Such VRBIS data and other personal and confidential information are also referred to herein collectively as "Protected Data.") This Agreement covers Protected Data in any medium (paper, electronic, oral) the Protected Data exist in.

By entering into this Agreement, CDPH and Data Recipient desire to protect the privacy and provide for the security of all Protected Data in compliance with all state and federal laws applicable to the Protected Data. Permission to receive, use and disclose Protected Data requires execution of this Agreement that describes the terms, conditions and limitations of Data Recipient's collection, use, and disclosure of the Protected Data.

I. **Supersession:** This Agreement supersedes Agreement Number None, dated None, between CDPH and Data Recipient.

II. **Definitions:** For purposes of this Agreement, the following definitions shall apply:

A. **Breach:** "Breach" means:

1. The acquisition, access, use, or disclosure of Protected Data, in any medium (paper, electronic, oral), in violation of any state or federal law or in a manner not permitted under this Agreement, that compromises the privacy, security, or integrity of the information. For purposes of this definition, "compromises the privacy, security or integrity of the information" means to pose a significant risk of financial, reputational, or other harm to an individual or individuals; or
2. The same as the definition of "breach of the security of the system" set forth in California Civil Code Section 1798.29(d).

B. **Confidential Information:** "Confidential Information" means information that:

1. Does not meet the definition of "public records" set forth in California Government Code Section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or
2. Meets the definition of "confidential public health record" set forth in California Health and Safety Code Section 121035, subdivision (c); or
3. Is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word "confidential" by CDPH.

C. **Disclosure:** "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information.

D. **Vital Records Business Intelligence System (VRBIS) Data:** "VRBIS data" means all California birth, death, and fetal death vital records data in and from the VRBIS database supported and maintained by CDPH. VRBIS data specifically includes information contained in or extracted from the following:

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

1. Statewide and County-Specific California birth and death data indices and files compiled by the State Registrar pursuant to California Health and Safety Code (H&SC) sections 102230 and 102231.
2. Birth Certificate and automated birth registration social and medical data collected pursuant to H&SC sections 102425, 102425.1, and 102426.
3. Death and Fetal Death Certificate social and medical data collected pursuant to H&SC sections 102875 and 103025.

E. Personal Information: “Personal Information” means information that:

1. By itself, directly identifies, or uniquely describes an individual; or
2. Creates a substantial risk that it could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or
3. Meets the definition of “personal information” set forth in California Civil Code section 1798.3, subdivision (a); or
4. Is one of the data elements set forth in California Civil Code section 1798.29, subdivisions (e)(1), (2) or (3); or
5. Meets the definition of “medical information” set forth in either California Civil Code section 1798.29, subdivision (f)(2) or California Civil Code section 56.05, subdivision (g); or
6. Meets the definition of “health insurance information” set forth in California Civil Code section 1798.29, subdivision (f)(3).

F. Protected Data: “Protected Data” means data that consists of one or more of the following types of information:

1. “VRBIS Data”, as defined above; or
2. “Confidential Information”, as defined above; or
3. “Personal Information”, as defined above.

G. Security Incident: “Security Incident” means:

1. An attempted breach; or
2. The attempted or successful modification or destruction of Protected Data, in violation of any state or federal law or in a manner not permitted under this Agreement; or
3. The attempted or successful modification or destruction of, or interference with, Data Recipient’s system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of Protected Data, or hinders or makes impossible Data Recipient’s receipt, collection, creation, storage, transmission or use of Protected Data by Data Recipient pursuant to this Agreement.

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

H. Use: “Use” means the sharing, employment, application, utilization, examination, or analysis of information.

III. Background and Purpose:

The CDPH and its Director, designated in statute as the State Registrar, pursuant to Division 102 of the California Health and Safety Code (H&SC), is charged with the duties of registering, maintaining, indexing and issuing certified copies of, all California Birth, Death, and Fetal Death records. As part of these activities, the State Registrar operates the VRBIS database. VRBIS is a secure, web based electronic solution for the State Registrar to store California’s vital records data and to permit Local Health Departments to access such data for purposes of official government business including epidemiologic analysis, surveillance, and program evaluation, as directed by the Local Health Officer, following all applicable laws and regulations concerning vital record data.

IV. Legal Authority for Use and Disclosure of Protected Data: The legal authority for CDPH to collect, use, and disclose Protected Data, and for Data Recipient to receive and use Protected Data is as follows:

A. General Legal Authority:

1. California Information Practices Act:

- a. California Civil Code section 1798.24(e), provides in part as follows: “No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed, as follows: To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected...”

B. Specific Legal Authority: Vital Records Collection, Use, and Dissemination

1. Division 102 of the H&SC designates that the Director of CDPH is the State Registrar and such duties include the registration, preservation, and dissemination of all of California’s birth, death and marriage records.
2. H&SC section 102230 designates that the State Registrar “shall arrange and permanently preserve the [vital records] certificates in a systematic manner and shall prepare and maintain comprehensive and continuous indices of all certificates registered. Further, H&SC section 102230 designates that the State Registrar, at his or her discretion, may release comprehensive birth and death indices to a government agency. A government agency that obtains indices shall not sell or release the index or a portion of its contents to another person except as necessary for official government business and shall not post the indices or any portion thereof on the Internet.
3. Pursuant to H&SC section 102430(a), the second section of the certificate of live birth as specified in subdivision (b) of H&SC section 102425, the electronic file of birth information collected pursuant to subparagraphs (B) to (F), inclusive, of paragraph (2) of subdivision (a) of H&SC section 102426, and the second section of the certificate of fetal death as specified in H&SC section 103025, are confidential; however, access to this information is authorized for the following: local registrar’s staff and local health department staff (when approved by the local registrar or local health officer, respectively) and the county coroner.

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

4. Pursuant to H&SC section 103526(c)(2)(C), authorized copies of birth and death certificates may be obtained by a representative of another governmental agency, as provided by law, who is conducting official business.

C. Health Insurance Portability and Accountability Act (HIPAA) Authority:

1. **CDPH HIPAA Status:** CDPH is a “hybrid entity” for purposes of applicability of the federal regulations entitled, “Standards for Privacy of Individually Identifiable Health Information,” (“Privacy Rule”) (Title 45, Code of Federal Regulations, Parts 160, 162, and 164) promulgated pursuant to HIPAA (Title 42, United States Code, Sections 1320d - 1320d-8). None of the CDPH programs that collect, use, or disclose Protected Data pursuant to this Agreement have been designated by CDPH as HIPAA-covered “health care components” of CDPH. (Title 45, Code of Federal Regulations, Section 164.504(c)(3)(iii).)
2. **Parties Are “Public Health Authorities:** CDPH and Data Recipient are each a “public health authority” as that term is defined in the Privacy Rule. (Title 45, Code of Federal Regulations, Sections 164.501 and 164.512(b)(1)(i).)
3. **Protected Data Use and Disclosure Permitted by HIPAA:** To the extent a disclosure or use of Protected Data is a disclosure or use of “Protected Health Information” (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Protected Data disclosure and/or use by CDPH and Data Recipient, without the consent or authorization of the individual who is the subject of the PHI:
 - a. The HIPAA Privacy Rule creates a special rule for a subset of public health disclosures whereby HIPAA cannot preempt state law if, “[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.” (Title 45, Code of Federal Regulations, Section 160.203(c).) [NOTE: See Sections IV.A and IV.B, above.];
 - b. A covered entity may disclose PHI to a “public health authority” carrying out public health activities authorized by law; (Title 45, Code of Federal Regulations, Section 164.512(b).); and
 - c. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific Protected Data uses and disclosures.

- V. **Disclosure Restrictions:** The Data Recipient, and its employees or agents, shall protect from unauthorized disclosure any Protected Data. The Data Recipient shall not disclose, except as specifically permitted by this Agreement, any Protected Data to anyone other than CDPH, except if disclosure is allowed or required by state or federal law.

- VI. **Use and VRBIS Access Restrictions:** The Data Recipient, and its employees or agents, shall not use any Protected Data for any purpose other than carrying out the Data Recipient's obligations under the statute set forth in Section IV, above, or as otherwise allowed or required by state or federal law.

CDPH will provide a unique username and password for each individual accessing the VRBIS secured database, on behalf of Data Recipient. Data Recipient shall be responsible for identifying one primary individual to be granted access. Data Recipient may request that a second individual be granted access to act as backup for the primary individual, or if workload constraints warrant a second individual's access. Data Recipient may submit a request to CDPH for a third VRBIS access username and password, with documentation justifying the need. These requests will be considered on a case-by-case

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

basis, and will take into consideration Data Recipient's business case for need as well as the limitations and burden of an additional user in VRBIS. If there are personnel changes to the Data Recipient's user account designees, Data Recipient shall immediately notify the CDPH VRBIS contact identified in Section XII(E), below, upon which time that user account shall be cancelled.

VII. Safeguards: Data Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Protected Data, including electronic or computerized Protected Data. The Data Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Data Recipient's operations and the nature and scope of its activities in performing its legal obligations and duties (including performance of its duties and obligations under this Agreement), and which incorporates the requirements of Section VIII, Security, below. Data Recipient shall provide CDPH with Data Recipient's current and updated policies.

VIII. Security: The Data Recipient shall take all steps necessary to ensure the continuous security of all computerized data systems containing Protected Data. These steps shall include, at a minimum:

- A. Complying with all of the data system security precautions listed in the Data Recipient Data Security Standards set forth in Attachment A to this Agreement;
- B. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

In case of a conflict between any of the security standards contained in any of the aforementioned sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to Protected Data from breaches and security incidents.

IX. Security Officer: The Data Recipient shall designate a Security Officer to oversee its compliance with this Agreement and for communicating with CDPH on matters concerning this Agreement.

X. Training: The Data Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its employees who assist in the performance of Data Recipient's obligations under this Agreement, or otherwise use or disclose Protected Data.

- A. The Data Recipient shall require each employee who receives training to sign a certification, indicating the employee's name and the date on which the training was completed.
- B. The Data Recipient shall retain each employee's written certifications for CDPH inspection for a period of three years following contract termination.

XI. Employee Discipline: Data Recipient shall discipline such employees and other Data Recipient workforce members who intentionally violate any provisions of this Agreement, including, if warranted, by termination of employment.

XII. Breach and Security Incident Responsibilities:

- A. Notification to CDPH of Breach or Security Incident: The Data Recipient shall notify CDPH **immediately by telephone call plus e-mail or fax** upon the discovery of a breach (as defined in this

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

Agreement), or within **24 hours by e-mail or fax** of the discovery of any security incident (as defined in this Agreement). Notification shall be provided to the VRBIS Project Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XII (E), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Protected Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Technology Service Desk at the telephone numbers listed in Section XII (E), below. For purposes of this section, breaches and security incidents shall be treated as discovered by Data Recipient as of the first day on which such breach or security incident is known to the Data Recipient, or, by exercising reasonable diligence would have been known to the Data Recipient. Data Recipient shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach or security incident, who is an employee or agent of the Data Recipient.

Data Recipient shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and
 2. Any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code Section 1798.29.
- B. Investigation of Breach: The Data Recipient shall immediately investigate such breach or security incident, and within 72 hours of the discovery, shall inform the VRBIS Project Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:
1. What data elements were involved and the extent of the data involved in the breach, including, specifically, the number of individuals whose personal information was breached; and
 2. A description of the unauthorized persons known or reasonably believed to have improperly used the Protected Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Protected Data, or to whom it is known or reasonably believed to have had the Protected Data improperly disclosed to them; and
 3. A description of where the Protected Data is believed to have been improperly used or disclosed; and
 4. A description of the probable causes of the breach or security incident; and
 5. Whether California Civil Code Section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.
- C. Written Report: The Data Recipient shall provide a written report of the investigation to the CDPH VRBIS Project Contact, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer within five working days of the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence of such breach or security incident.
- D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Data Recipient is considered only a custodian

VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS) DATA USE AND DISCLOSURE AGREEMENT

and/or non-owner of the Protected Data, Data Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. Make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. The CDPH Privacy Officer shall approve the time, manner and content of any such notifications, prior to the transmission of such notifications to the individuals; or
 2. Cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.
- E. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Data Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Data Recipient. Said changes shall not require an amendment to this Agreement.

CDPH VRBIS Project Contact	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
CA-VRBIS Project Support Desk / Laura Lund 1501 Capitol Ave. MS 5101 P.O. Box 997410 Sacramento, CA 95899-7410 Laura.Lund@cdph.ca.gov Telephone: (916) 552-8113	Privacy Officer Privacy Office, Office of Legal Services, CDPH 1415 L Street, Suite 500 Sacramento, CA 95814 privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office, CDPH, MS 6302 P.O. Box 997377 Sacramento, CA 95899-7377 cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

- XIII. Indemnification: Data Recipient shall indemnify, hold harmless and defend CDPH from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorneys' fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Data Recipient, its officers, employees or agents relative to the Protected Data, including without limitation, any violations of Data Recipient's responsibilities under this Agreement.
- XIV. Term of Agreement: This Agreement shall remain in effect for three (3) years after the last signature date in the signature block below. After three (3) years, this Agreement will expire without further action. If the parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement. The newly signed agreement should explicitly supersede this Agreement, which should be referenced by Agreement Number and date in Section I of the new Agreement. If one or both of the parties wish to terminate this Agreement prematurely, they may do so upon 30 days advanced notice. CDPH may also terminate this Agreement pursuant to Section XV or XVII, below.
- XV. Termination for Cause:
- A. Termination Upon Breach: A breach by Data Recipient of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreement by CDPH. At its sole discretion, CDPH may give Data Recipient 30 days to cure the breach.

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

- B. Judicial or Administrative Proceedings: Data Recipient will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CDPH may terminate the Agreement if Data Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate the Agreement if a finding or stipulation that the Data Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which the Data Recipient is a party or has been joined.
- XVI. Return or Destruction of Protected Data on Expiration or Termination: On expiration or termination of the agreement between Data Recipient and CDPH for any reason, Data Recipient shall return or destroy the Protected Data. If return or destruction is not feasible, Data Recipient shall explain to CDPH why, in writing, to the VRBIS Project Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII (E), above.
- A. Retention Required by Law: If required by state or federal law, Data Recipient may retain, after expiration or termination, Protected Data for the time specified as necessary to comply with the law.
- B. Obligations Continue Until Return or Destruction: Data Recipient's obligations under this Agreement shall continue until Data Recipient destroys the Protected Data or returns the Protected Data to CDPH; provided however, that on expiration or termination of the Agreement, Data Recipient shall not further use or disclose the Protected Data except as required by state or federal law.
- C. Notification of Election to Destroy Protected Data: If Data Recipient elects to destroy the Protected Data, Data Recipient shall certify in writing, to the VRBIS Project Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII (E), above, that the Protected Data has been destroyed.
- XVII. Amendment: The parties acknowledge that federal and state laws relating to information security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of Protected Data. Upon CDPH request, Data Recipient agrees to promptly enter into negotiations with CDPH concerning an amendment to this Agreement embodying written assurances consistent with new standards and requirements imposed by regulations and other applicable laws. CDPH may terminate this Agreement upon 30-days written notice in the event:
- A. Data Recipient does not promptly enter into negotiations to amend this Agreement when requested by CDPH pursuant to this section; or
- B. Data Recipient does not enter into an amendment providing assurances regarding the safeguarding of Protected Data that CDPH in its sole discretion deems sufficient to satisfy the standards and requirements of applicable laws and regulations relating to the security or privacy of Protected Data.
- XVIII. Assistance in Litigation or Administrative Proceedings: Data Recipient shall make itself and any employees or agents assisting Data Recipient in the performance of its obligations under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Data Recipient, except where Data Recipient or its employee or agent is a named adverse party.

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

- XIX. **Disclaimer:** CDPH makes no warranty or representation that compliance by Data Recipient with this Agreement will be adequate or satisfactory for Data Recipient's own purposes or that any information in Data Recipient's possession or control, or transmitted or received by Data Recipient, is or will be secure from unauthorized use or disclosure. Data Recipient is solely responsible for all decisions made by Data Recipient regarding the safeguarding of Protected Data.
- XX. **Transfer of Rights:** Data Recipient has no right and shall not subcontract, delegate, assign, or otherwise transfer or delegate any of its rights or obligations under this Agreement to any other person or entity. Any such transfer of rights shall be null and void.
- XXI. **No Third-Party Beneficiaries:** Nothing expressed or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Data Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities, whatsoever.
- XXII. **Interpretation:** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State and Federal laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with federal and state laws.
- XXIII. **Survival:** The respective rights and obligations of Data Recipient under Sections VII, VIII and XII of this Agreement shall survive the termination or expiration of this Agreement .
- XXIV. **Entire Agreement:** This Agreement constitutes the entire agreement between CDPH and Data Recipient. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.
- XXV. **Severability:** The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.
- XXVI. **Signatures:**

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of the Data Recipient, the _____ Local Health Department, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

(Name of Representative of the Local Health Department)

(Title)

(Signature)

(Date)

**VITAL RECORDS BUSINESS INTELLIGENCE SYSTEM (VRBIS)
DATA USE AND DISCLOSURE AGREEMENT**

On behalf of CDPH, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

(Name of CDPH Representative)

(Title)

(Signature)

(Date)

Attachment A
Data Recipient Data Security Standards

1. General Security Controls

- a. **Confidentiality Statement.** All persons that will be working with Protected Data must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Protected Data. The statement must be renewed annually. The Data Recipient shall retain each person's written confidentiality statement for CDPH inspection for a period of three years following contract termination.
- b. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- c. **Server Security.** Servers containing unencrypted Protected Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- d. **Minimum Necessary.** Only the minimum necessary amount of Protected Data required to perform necessary business functions may be copied, downloaded, or exported.
- e. **Removable media devices.** All electronic files that contain Protected Data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, Blackberry, back-up tapes, etc.). Must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher.
- f. **Antivirus software.** All workstations, laptops, and other systems that process and/or store Protected Data must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- g. **Patch Management.** All workstations, laptops, and other systems that process and/or store Protected Data must have security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- h. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Protected Data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords: are not to be shared; must be at least eight characters; must be a non-dictionary word; must not be stored in readable format on the computer; must be changed every 60 days; must be changed if revealed or compromised and must be composed of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z);
 - Lower case letters (a-z);
 - Arabic numerals (0-9); and
 - Non-alphanumeric characters (punctuation symbols).
- i. **Data Sanitization.** All Protected Data must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. System Security Controls

- a. **System Timeout.** The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- b. **Warning Banners.** All systems containing Protected Data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
- c. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Protected Data, or which alters Protected Data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Protected Data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.
- d. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.
- e. **Transmission encryption.** All data transmissions of Protected Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing Protected Data can be encrypted. This requirement pertains to any type of Protected Data in motion such as website access, file transfer, and e-mail.
- f. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Protected Data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

- a. **System Security Review.** All systems processing and/or storing Protected Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.
- b. **Log Reviews.** All systems processing and/or storing Protected Data must have a routine procedure in place to review system logs for unauthorized access.
- c. **Change Control.** All systems processing and/or storing Protected Data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity/Disaster Recovery Controls

- a. **Disaster Recovery.** Data Recipient must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Protected Data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.
- b. **Data Backup Plan.** Data Recipient must have established documented procedures to back-up Protected Data to maintain retrievable exact copies of Protected Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of back-up media, and the amount of time to restore Protected Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. Paper Document Controls

- a. **Supervision of Data.** Protected Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Protected Data in paper form shall not be left unattended at any time in vehicles, planes, trains, or any other modes of transportation and shall not be checked in baggage on commercial airplanes.
- b. **Escorting Visitors.** Visitors to areas where Protected Data is contained shall be escorted and CDPH PHI shall be kept out of sight while visitors are in the area.
- c. **Confidential Destruction.** Protected Data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.
- d. **Removal of Data.** Protected Data must not be removed from the premises of the Data Recipient except with express written permission of CDPH.
- e. **Faxing.** Faxes containing Protected Data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.
- f. **Mailing.** Protected Data shall only be mailed using secure methods. Large volume mailings of CDPH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH-approved solution, such as a solution using a vendor product specified on the CSSI.